UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

DAVID DE MEDICIS, on behalf of himself and all others similarly situated, Plaintiff, v. ALLY BANK and ALLY FINANCIAL INC., Defendants.	Case No. 21-cv-6799-NSR ORAL ARGUMENT REQUESTED

MEMORANDUM OF LAW IN SUPPORT OF
DEFENDANTS' MOTION TO DISMISS THE COMPLAINT

SIMPSON THACHER & BARTLETT LLP
425 Lexington Avenue
New York, New York 10017
Telephone: (212) 455-2000
Facsimile: (212) 455-2502

Attorneys for Defendants Ally Bank and Ally Financial Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Defendants Ally Bank and Ally Financial Inc. (together, "Ally" or "Defendants"), by and through their undersigned counsel, respectfully submit this memorandum of law in support of their motion to dismiss the Class Action Complaint ("Complaint") of Plaintiff David De Medicis ("Plaintiff") pursuant to Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction and Rule 12(b)(6) for failure to state a claim upon which relief can be granted.

PRELIMINARY STATEMENT

This case involves an inadvertent computer "programming code error" that occurred when some customers logged into Ally's website. The error, which happened only under certain circumstances and not in every instance of a customer login, caused a lengthy string of characters, which had usernames and passwords embedded in the string, to be transmitted electronically to certain businesses that perform services for Ally (each of which is known to and maintains an ongoing relationship with Ally). Immediately after discovering the error, Ally fixed the code and forced all potentially-impacted passwords to be reset. Additionally, each of the businesses that work with Ally agreed to and then deleted the information. Ally also immediately began and continues to engage in fraud-monitoring efforts. Ally's prompt response was successful—not a single instance of identity theft or similar fraud attributable to the error has been identified. Put simply, the inadvertent error has not caused any cognizable harm to any of Ally's customers.

Nevertheless, Plaintiff filed this putative class action. The Complaint does not, however, allege that Plaintiff has suffered any concrete harm. Rather, he seeks relief for the *speculative* and *theoretical* threat of future injury. Tellingly, while Plaintiff refers to this case as involving a "data breach," he acknowledges that it actually involves an "inadvertent" error that "did not result from a sophisticated attack perpetrated by cybercriminals or state sponsored hackers." Compl. ¶¶ 1, 3. It is thus not surprising—especially in light of the proactive steps taken by Ally—that Plaintiff

alleges no actual injury resulting from the inadvertent error. In essence, Plaintiff asks this Court to impose liability on Ally simply because the error occurred. That is not the law, and established Supreme Court and Second Circuit law confirm the Complaint should be dismissed.

First, Plaintiff's Complaint should be dismissed under Rule 12(b)(1) because Plaintiff lacks Article III standing and thus this Court lacks subject matter jurisdiction. Article III standing requires either a present injury or a substantial likelihood of future injury. Plaintiff has pled neither. As to present injury, Plaintiff has not identified any fraud, identity theft, or other harm resulting from the inadvertent error, and his allegations of "time spent" monitoring his accounts and changing his passwords on an email account (*not* his Ally account) are insufficient as a matter of law. *See Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021) ("No concrete harm, no standing."). As to future injury, Plaintiff fails on all three of the factors the Second Circuit identified earlier this year as determinative in cases involving the unauthorized exposure of data and premised on a theory of future harm; specifically, (i) the exposure was due to an inadvertent error rather than to malicious hackers, (ii) the exposed information has not been misused, and (iii) the exposed information was not sensitive or high risk (and could easily be made useless by changing it). *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021). Because Plaintiff has not alleged injury in fact, this Court lacks subject matter jurisdiction.

Second, even if Plaintiff had standing (he does not), each of his five claims should be dismissed under Rule 12(b)(6) for failure to state a claim. First, the negligence claim fails because neither Utah nor Virginia (the jurisdictions relevant to Plaintiff's common-law claims) would recognize a duty in these circumstances, and Plaintiff has not pled a lack of reasonable care or actual damages. Second, the negligence *per se* claim, premised on Section 5 of the Federal Trade Commission Act, fails because Utah permits negligence *per se* claims only in cases involving

dangerous instrumentalities, and Virginia permits negligence *per se* claims only where predicated on statutes enacted for public safety, neither of which is alleged here. Third, the implied contract claim fails because Plaintiff does not allege an enforceable agreement under either Utah or Virginia law and fails to allege any economic damages. Fourth, the Virginia Personal Information Breach Notification Act claim fails because, as defined by the statute, the inadvertent error did not involve Plaintiff's "personal information," was not a "breach," and Plaintiff has not pled any unreasonable delay in being notified of the error. Fifth, the claim for declaratory or injunctive relief fails because Plaintiff's underlying claims are invalid, and there is no substantial risk of future harm to enjoin.

Under either Rule 12(b)(1) or 12(b)(6), the Complaint should be dismissed.

RELEVANT FACTUAL BACKGROUND

A. The parties.

Ally Financial Inc. is a leading digital financial-services company that provides a variety of financial services to more than 8.5 million consumer, commercial, and corporate customers. Its wholly-owned subsidiary, Ally Bank, is an award-winning digital direct bank that offers mortgage lending, point-of-sale personal lending, and a variety of other banking and investment products.[1]

Plaintiff "is a Virginia resident." Compl. ¶ 12. He maintains "checking, savings and securities accounts" with Ally. *Id.*[2]

B. The Coding Error.

On April 12, 2021, during a routine website update, Ally learned of an inadvertent coding error that affected certain query strings that transmit information after a customer entered a username and password to access an Ally account (the "Coding Error"). Compl. ¶¶ 22, 24; Decl.

[1] *See* 2020 10-K Annual Report, Ally Financial Inc. (Feb. 24, 2021) at 5.

[2] Plaintiff does not allege that his claims are based on accounts with Ally Invest. To the extent Plaintiff seeks to assert any claims based on his Ally Invest account, such claims are subject to mandatory and binding arbitration.

¶ 3.[3] These query strings—which send information across Ally's platform to allow customers to access their online accounts—usually do not contain any personally identifiable information. Decl. ¶¶ 4–5. The Coding Error, however, resulted in certain query strings that potentially contained usernames and passwords (embedded within the string of code) being sent to a limited group of known entities with which Ally has ongoing contractual and business relationships. *Id.* ¶ 6.[4] The following is an actual (redacted) query string:

> https://www.ally.com,/,/,/?hdmjavascriptdata=&allysf-login-v1-account=aaos&allysf-login-v1-username-78e30d704ccce8ccc7b8539f0144cb09=[redacted]&allysf-login-v1-password-78e30d704ccce8ccc7b8539f0144cb09=[redacted]

Id. ¶ 9. The Coding Error only occurred in limited circumstances where the user attempted to log in before the page had fully loaded (*e.g.*, if the user was using software to automatically populate the username and password). *Id.* ¶ 6.

In order to actually access an Ally online account, a person at one of the entities to which the strings were visible would have had to first ascertain that a query string *could* have included a username and password, and would then have had to parse the information from within the string. *Id.* ¶ 8. Not all usernames and passwords in the query strings, moreover, would have necessarily contained correct or complete usernames or passwords; for example, if a customer had incorrectly typed the username or password, that incorrect information would have been embedded in the string, and the information could not be used to gain access to an account. *Id.*

C. Ally eliminates the Coding Error and assesses the potential impact.

Immediately upon learning of the Coding Error, Ally updated the affected code to eliminate

---

[3] Citations to "Decl. ¶ __" refer to the Declaration of Christian Hall, submitted herewith.

[4] Ally engages these entities to assist with user experience on Ally's website and marketing efforts. Ally intended to transmit limited data, including query strings, to these businesses as part of Ally's ongoing business and established protocols with these entities. Decl. ¶ 7. These relationships are both direct and indirect—*i.e.*, a third party that Ally engages directly might engage another party to perform a portion of the work requested by Ally. *Id.* ¶ 11.

the error. Compl. ¶ 24; Decl. ¶ 12. Ally also implemented a process that required all *potentially* affected customers—whether or not they were *actually* affected—to change their password. Decl. ¶ 13.

Additionally, Ally immediately began working with the businesses to which the query strings may have been visible to purge the information. *Id.* ¶ 14. All of these entities agreed to delete the information, and all subsequently confirmed deletion. *Id.*

Ally also immediately began the process of determining which customers' usernames and passwords may have been embedded in the query strings as a result of the Coding Error. *Id.* ¶ 16. To do this, Ally had to parse through millions of website login attempts and, for each login attempt, identify whether the Coding Error had actually occurred during the login attempt (because, as noted above, it only occurred in certain circumstances) and, if so, match the information to a specific customer. *Id*. Ultimately, Ally identified each of its customers who could have been potentially impacted by the Coding Error. *Id.* ¶ 17.

Ally also immediately began fraud-monitoring efforts to assess threats or risks of fraud specific to the Coding Error, including monitoring the accounts of potentially-affected customers for fraudulent, suspicious, or anomalous activity. *Id.* ¶ 15.

D. Ally promptly notifies potentially impacted customers of the Coding Error.

After identifying which customers' information had been embedded in the query strings as a result of the Coding Error, Ally sent each customer a letter explaining the circumstances of the error. *Id.* ¶ 18. This letter, dated June 11, 2021, explained the remedial steps that Ally had taken as quickly as possible after discovering the Coding Error, including (1) updating the code; (2) requiring customers to reset their passwords; (3) confirming that all third parties would delete the information; and (4) monitoring customers' accounts. *See* Compl. ¶¶ 1, 12; *see also* Decl. ¶¶ 18, 20, Ex. A (copy of letter sent to Plaintiff). Additionally, although the risk of potential fraud

was low given the circumstances of the Coding Error and the steps that Ally immediately took, Ally offered all affected customers with free credit monitoring and identity theft insurance coverage for two years. Compl. ¶ 10; Decl. ¶ 19, Ex. A.

E. Ally identifies no fraudulent activity as a result of the Coding Error.

Since discovery of the Coding Error on April 12, 2021, Ally's internal cyber risk and fraud teams have monitored the accounts of the customers affected by the Coding Error for any increase in potential fraudulent or other anomalous activity. Decl. ¶ 21. Ally has identified *no* instances of account takeovers, identity theft, or similar occurrences attributable to the Coding Error. *Id.* ¶ 22. Additionally, Ally has not identified any increased rates of potentially fraudulent activity or other anomalous events attributable to the Coding Error; in other words, the rate of potentially fraudulent activity across the population of affected accounts has remained in line with that of *un*affected customer accounts. *Id.*[5]

F. The Complaint.

On August 12, 2021, Plaintiff filed the Complaint, alleging five causes of action: negligence, negligence *per se*, breach of implied contract, violation of the Virginia Personal Information Breach Notification Act, and injunctive/declaratory relief under the Declaratory Judgment Act. *See* Compl. ¶¶ 60–99. Plaintiff claims he was "harmed" by the Coding Error because he "devot[ed] time" to "self-monitoring his accounts" and "changing the password and usernames on many of his personal online accounts," and suffered "diminution in the value of his private information" as well as "lost time, annoyance . . . and inconvenience." *Id.* ¶¶ 32–34. Plaintiff also alleges he has experienced "three attempts by hackers to reset the password of his

[5] As the government sources Plaintiff cites in the Complaint (*see* Compl. ¶¶ 44–46) make clear, it is well known that rates of potential fraudulent activity is never zero. *See, e.g.*, U.S. Government Accountability Office, Report to Congressional Requestors (June 2007), at 19 (cited at Compl. ¶ 46).

email account without his knowledge or permission." *Id.* ¶ 51.

ARGUMENT

I. THE COMPLAINT SHOULD BE DISMISSED UNDER RULE 12(b)(1) BECAUSE PLAINTIFF LACKS ARTICLE III STANDING.

A. Legal standard.

Dismissal is proper under Rule 12(b)(1) for lack of subject matter jurisdiction where the plaintiff lacks Article III standing because "[i]f plaintiffs lack Article III standing, a court has no subject matter jurisdiction to hear their claim." *Cent. States So. & Sw. Areas Health & Welfare Fund v. Merck-Medco Managed Care, L.L.C.*, 433 F.3d 181, 198 (2d Cir. 2005). "A plaintiff asserting subject matter jurisdiction has the burden of proving by a preponderance of the evidence that jurisdiction exists." *Clarex Ltd. v. Natixis Secs. Am. LLC*, 2012 WL 4849146, at *2 (S.D.N.Y. Oct. 12, 2012) (noting that "jurisdiction must be shown affirmatively").

A 12(b)(1) motion to dismiss can be facial (*i.e.*, based solely on the allegations in the complaint), or fact-based (*i.e.*, based on proffered evidence beyond the complaint). *See Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 56–57 (2d Cir. 2016). On a facial motion, the court "determine[s] whether the [complaint] allege[s] facts that affirmatively and plausibly suggest that [the plaintiff] has standing to sue." *Id.* On a factual motion, defendants may submit factual declarations, and the plaintiff "will need to come forward with evidence of [his] own to controvert" defendants' evidence. *Id*. at 57. If defendants' evidence is "material and controverted," the court must make factual findings to determine whether the plaintiff has standing. *Id*.

To establish "the irreducible constitutional minimum" of Article III standing, a plaintiff must demonstrate (1) "an injury in fact to a legally protected interest that is both concrete and particularized, and *actual or imminent*, not conjectural or hypothetical"; (2) that the defendant caused the injury; and (3) that it is "likely" that the requested relief would "redress" the injury.

See Crupar-Weinmann v. Paris Baguette Am., Inc., 861 F.3d 76, 79 (2d Cir. 2017) (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). To satisfy the "injury in fact" element in cases involving allegations of "unauthorized exposure of th[e] plaintiff's data," the complaint must establish either a *present* injury or a *future* injury due to the alleged exposure. *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 300–01 (2d Cir. 2021). A future injury may satisfy the "injury in fact" requirement "only if the threatened injury is *certainly impending*, or if there is a *substantial risk* that the harm will occur." *Id.* (emphases added).

B. Plaintiff fails to allege—and cannot demonstrate—a *present* injury.

Plaintiff cannot demonstrate the requisite concrete, particularized, present injury in fact. The Complaint does not allege that the Coding Error resulted in any actual misuse of Plaintiff's username and password. Instead, Plaintiff's *only* allegations of present injury are (1) "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts (Compl. ¶¶ 31–32); (2) "diminution in the value" of Plaintiff's private information (*id.* ¶ 33); and (3) "three attempts by hacker[s] to reset the password of his email account without his knowledge or permission" (*id*. ¶ 51). As a matter of law, the time Plaintiff allegedly spent monitoring his online accounts cannot constitute an injury in fact in the absence of a substantial risk of future identity theft—which simply does not exist here. *See infra* Section I.C.4. Plaintiff's other allegations of present injury likewise fail.

Alleged diminution in value. Plaintiff's allegation that he has "suffered" "diminution in the value of his [p]rivate [i]nformation" (Compl. ¶ 33) is insufficient because he has not—and cannot—allege that there is a market for his so-called "private information," nor that disclosure of that information decreased its market value. *E.g.*, *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *8 (S.D.N.Y. March 23, 2021) (allegations of lost value in private information "are actionable *only if* the plaintiff also alleges the existence of a market for that information and how

the value of such information could have decreased due to its disclosure"); *see also, e.g.*, *Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016) ("Courts have routinely rejected the proposition that an individual's personal identifying information has an independent monetary value."); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (alleged "loss of [plaintiffs'] private information" is an "abstract injury" that cannot "support[] standing," "particularly since the complaint does not suggest that the plaintiffs could sell their personal information for value").

Plaintiff does not allege that there is any market for his "personal information," nor that the value of his personal information decreased as a result of the Coding Error. Indeed, the Complaint does not allege that Plaintiff's information (or any other Ally customers' information) was sold to hackers or other nefarious parties. As a practical matter, this is unsurprising because—unlike a Social Security Number, birthdate, or other sensitive personal information—there is nothing inherently valuable about a username and password, both of which are selected by the user and can be easily changed at a moment's notice. *See Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90–91 (2d Cir. 2017) (summary order) (plaintiff lacked Article III standing because, among other reasons, the risk of future identity theft was eliminated by cancelling the stolen credit card). Although Plaintiff alleges generally that access to an Ally account could lead to access to sensitive personal information (*see* Compl. ¶ 28), the Complaint does not allege that any such access ever *actually occurred* with respect to his or any other Ally customer's account. Thus, even assuming a market for Plaintiff's information, the Complaint does not allege any facts from which the Court could plausibly infer that the Coding Error decreased its value. *See, e.g.*, *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017) ("Because Plaintiffs have not alleged any facts regarding how the data breach has led to a diminution in the value of their personal information, there can be no standing on this basis.").

"Attempts" to access Plaintiff's email account. Plaintiff alleges that since the Coding Error, "on three separate occasions, Plaintiff has encountered *attempts* by *hacker* [sic] to reset the password of his email account without his knowledge or permission." Compl. ¶ 51 (emphasis added). Plaintiff's implicit admission that these alleged attempts to access his email were unsuccessful is sufficient to find no actual or present injury. *See Transunion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021) ("No concrete harm, no standing."); *Whalen*, 689 F. App'x at 90 (attempted fraud insufficient to constitute injury). Moreover, Plaintiff alleges no plausible link between the Coding Error and these alleged attempts to reset the password for his email account (*not* his Ally account); the only (implicitly) alleged connection is that the alleged attempts happened *after* the Coding Error. Plaintiff's argument is essentially that the *fact* of the Coding Error means he suffered an injury—even if he suffered *no actual harm*. The U.S. Supreme Court has squarely rejected this argument: "Under Article III, an injury in law is not an injury in fact." *Transunion*, 141 S. Ct. at 2205. Thus, even where a defendant has violated a statute (which is not the case here), "only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation [have standing to] sue . . . over that violation in federal court." *Id.*[6] (emphasis added).

Plaintiff has not—and cannot—demonstrate a concrete and present injury in fact.

C. Plaintiff fails to allege—and cannot demonstrate—a substantial risk of *future* injury.

Plaintiff also has not, and cannot, demonstrate a substantial risk of a future injury in fact.

---

[6] The *Transunion* Court explained that "[c]entral to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms including (as relevant [in *Transunion*]) reputational harm." *Id*. at 2200 (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340–341 (2016)). In *Transunion*, the Supreme Court held that plaintiffs who were falsely flagged on their credit reports as being potential terrorists, drug traffickers, and the like had not suffered an injury in fact, and thus did not have standing, unless that incorrect and potentially damaging credit report had been provided to third-party businesses. *Id.* at 2201. This is because that additional factor constituted a concrete injury akin to defamation based on being wrongly labeled to third-party businesses with which plaintiffs were seeking a credit relationship (*e.g.*, car dealerships, etc.) as a threat to national security. *Id.* at 2209.

Plaintiff alleges that he has an "imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse." Compl. ¶¶ 30, 35. But his allegations about future injury are insufficient as a matter of law under binding Second Circuit precedent. *See McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021).

In *McMorris*, the Second Circuit held (but did not find) that Article III standing in an "unauthorized data disclosure" action could be based on a "substantial risk of future identity theft or fraud." *Id.* at 300, 303 ("[A] future injury constitutes an Article III injury in fact only 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" (quoting *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014))). The court distilled from its own and other circuits' precedent three factors that "bear on whether the risk of identity theft or fraud is sufficiently 'concrete, particularized, and . . . imminent'" for purposes of Article III standing in data-exposure cases: whether (1) "the plaintiffs' data has been exposed as the result of a *targeted* attempt to obtain that data" (emphasis added); (2) "any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud"; and (3) "the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud." *Id.* at 303. Here, each of the *McMorris* factors weighs heavily against Plaintiff.

1. The Coding Error was inadvertent, not the result of a targeted attack.

As to the first—and most important (*id*. at 301)—*McMorris* factor, Plaintiff acknowledges that the Coding Error was "inadvertent" and the result of a "'programming' error in [Ally's] customer website" rather than a "sophisticated attack perpetrated by cyber criminals or state sponsored hackers." Compl. ¶¶ 1–3, 12, 63. This disposes of the first factor. "Where plaintiffs fail to present evidence or make any allegations that an unauthorized third party purposefully obtained the plaintiffs' data, courts have regularly held that the risk of future identity theft is too speculative to support Article III standing." *McMorris*, 995 F.3d at 301 (collecting cases).

2. The transmitted information has not been misused.

As to the second *McMorris* factor, and as discussed *supra* Section I.B, the Complaint contains no allegations that the Coding Error resulted in *actual* misuse of Plaintiff's (or any other Ally customer's) username and password. Indeed, the Complaint does not include a single allegation that there has been any actual or attempted identity theft or fraud associated with Plaintiff's *Ally* accounts (alleged attempts to reset his *email* password, with nothing more, do not rise to this level). Nor does the Complaint allege that any of the information has been or is for sale. This disposes of the second factor. *See McMorris*, 995 F.3d at 301–02 (plaintiff must "show that at least some part of the compromised dataset has been misused," that "plaintiffs' data is already being misused," or that "the plaintiffs' [information] was for sale on the Dark Web").

Having not alleged any actual misuse, Plaintiff must rely on potential *future* misuse. But this theory does not help him, as it is not only speculative but also requires the Court to infer the type of implausible, "attenuated chain of possibilities" that the *McMorris* court rejected. *Id.* at 304. To find that Plaintiff has alleged a substantial risk of future harm stemming from the Coding Error, this Court would have to assume—notwithstanding that Plaintiff has not alleged any fraudulent activity or identity theft attributable to the Coding Error—that (a) a bad actor at one of the business entities that received the query strings figured out that these query strings included possible usernames and passwords; (b) the bad actor intentionally parsed the strings for this information; (c) the bad actor was actually able to access Plaintiff's account; (d) that the bad actor obtained information from Plaintiff's account that could be used for fraud or identity-theft purposes; and (e) the bad actor might someday use the information in a way that might injure Plaintiff. *See, e.g.*, Compl. ¶¶ 37, 47. This chain of events is speculative and implausible, both facially and factually. *See* Decl. ¶¶ 6–8. "[N]o Article III standing exists if a plaintiff's theory of injury rests on an 'attenuated chain of inferences necessary to find harm.'" *Cohen v. Ne.*

Radiology, P.C., 2021 WL 293123, at *4 (S.D.N.Y. Jan. 28, 2021) ("[A] 'subjective fear' or 'speculative threat' is not enough to identify injury." (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 415 n.5 (2013))).

3. The transmitted information was neither "sensitive" nor "high risk".

As to the third *McMorris* factor, as Plaintiff rightly concedes, it was his username and password—not sensitive and actionable personally identifiable information such as his name, birthdate, and Social Security Number—that was potentially made visible to certain third parties as a result of the Coding Error. *See* Compl. ¶ 1. This disposes of the third factor: exposure of usernames and passwords does not present a high risk of identity theft or fraud because both can easily be changed. Indeed, upon discovery of the Coding Error, Ally immediately forced all potentially affected customers to reset their passwords. Decl. ¶ 13. In contrast to the "dissemination of high-risk information such as Social Security numbers and dates of birth, especially when accompanied by victims' names," which "makes it more likely that those victims will be subject to future identity theft or fraud," less sensitive information, such as "data that can be rendered useless to cybercriminals[,] does not pose the same risk of future identity theft or fraud to plaintiffs if exposed." *McMorris*, 995 F.3d at 301–02 (ability to cancel credit card meant plaintiff did not "plausibly face a threat of future fraud" and thus lacked Article III standing); *see also, e.g.*, *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1344 (11th Cir. 2021) (same).

4. In the absence of a substantial risk of future injury, the time Plaintiff allegedly spent monitoring his accounts is not an injury in fact.

McMorris is also instructive with respect to Plaintiff's allegations regarding his "time spent" monitoring his accounts, "exploring credit monitoring and identity theft protection," and changing his passwords and usernames on various online accounts. Compl. ¶¶ 31–32. While these allegations are about *present* harm, *McMorris* and other courts evaluate such allegations in the

context of *future* harm—*i.e.*, only where a plaintiff has "shown a substantial risk of future identity theft or fraud [will] any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact." *McMorris*, 995 F.3d at 303. In contrast, where a plaintiff has "not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat *cannot* create an injury." *Id.* ("[W]here plaintiffs take steps to protect themselves following an unauthorized data disclosure, *can the cost of those proactive measures alone constitute an injury in fact*? . . . [T]he answer is '*no*.'" (emphasis added)). Under clear Supreme Court precedent, a plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.* (quoting *Clapper*, 568 U.S. at 416). As shown above, there is no substantial risk of future injury here. *See supra* Section I.C.1–3. Plaintiff thus cannot manufacture standing by alleging he "spent time" monitoring his accounts after the Coding Error.[7]

* * *

Plaintiff has neither a present injury nor a substantial risk of a future injury. Without injury, Plaintiff necessarily fails on the other elements of Article III standing. *See TransUnion*, 141 S. Ct. at 2203 (where "plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve"). Accordingly, the Complaint should be dismissed for lack of subject matter jurisdiction.[8]

II. THE COMPLAINT SHOULD BE DISMISSED UNDER RULE 12(b)(6) BECAUSE PLAINTIFF FAILS TO STATE ANY CLAIM FOR RELIEF.

Even if Plaintiff had standing, which he does not, each of Plaintiff's five claims should be dismissed under Rule 12(b)(6) for failure to state a claim.

---

[7] In any event, Ally offered Plaintiff two years of free credit monitoring. Decl. ¶ 19, Ex. A.

[8] Because Plaintiff lacks Article III standing, he also lacks standing to bring claims on behalf of the putative class. *See, e.g.*, *Jantzer v. Elizabethtown Comm. Hosp.*, 2020 WL 2404764, at *3 (N.D.N.Y. May 12, 2020).

A. Legal standard.

To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain "plausible" factual allegations, taken as true, which "raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "The plausibility standard . . . asks for more than a sheer possibility . . . Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The Court need not accept "'legal conclusions,' and '[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.'" *Harris v. Mills*, 572 F.3d 66, 72 (2d Cir. 2009) (quoting *Iqbal*, 556 U.S. at 678).

B. Choice of law.

Three of Plaintiff's five claims purport to allege violations of state common-law causes of action: negligence (Count I); negligence *per se* (Count II); and breach of implied covenant (Count III). A federal court sitting in diversity "applies the choice-of-law rules of the state in which it sits." *Andrews v. Sotheby Int'l Realty, Inc.*, 2014 WL 626968, at *4 (S.D.N.Y. Feb. 18, 2014), *aff'd*, 586 F. App'x 76 (2d Cir. 2014). New York's choice-of-law rules look to the state with the most significant interest in the litigation. *GlobalNet Financial.com, Inc. v. Frank Crystal & Co.*, 449 F.3d 377, 382 (2d Cir. 2006). For tort claims, this analysis is "almost exclusively" based on "the parties' domiciles and the locus of the [alleged] tort." *In re Thelen LLP*, 736 F.3d 213, 219–20 (2d Cir. 2013); *see also AEI Life LLC v. Lincoln Benefit Life Co.*, 892 F.3d 126, 135 (2d Cir. 2018) (similar for contract claims). In cases alleging unauthorized data disclosure, courts generally apply the law of the state in which the company is headquartered. *See Schmitt v. SN Serv. Corp.*, 2021 WL 3493754, at *4 (N.D. Cal. Aug. 9, 2021) (collecting cases).

The jurisdictions relevant to Plaintiff's claims are Utah—where Ally Bank, which is the

Defendant with which Plaintiff alleges he has his accounts, is headquartered—and Virginia—Plaintiff's domicile. *See* Compl. ¶ 12. The Court need not decide which law applies, however, because Plaintiff's claims fail under either Utah or Virginia law.[9]

C. Plaintiff fails to state a negligence claim (Count I).

Plaintiff claims that "[b]y collecting and storing [Plaintiff's] data, and using it for commercial gain, Ally had a duty of care to use reasonable means to secure and safeguard this private information." Compl. ¶ 62. The Coding Error constitutes negligence, Plaintiff claims, as it was due to "lack of reasonable care in programming, testing, and monitoring [Ally's] website." *Id.* ¶¶ 66–69. To state a negligence claim under either Utah or Virginia law, Plaintiff must adequately allege the existence of a legal duty of care, breach of that duty (*i.e.*, failure to use reasonable care), and that Plaintiff suffered actual damages. *See Hunsaker v. State*, 870 P.2d 893, 897 (Utah 1993); *Atrium Unit Owners Ass'n v. King*, 585 S.E.2d 545, 548 (Va. 2003).

1. Plaintiff cannot allege breach of an assumed duty.

Plaintiff does not (and could not) allege that Ally had a legal duty to him absent an *assumption* of duty by Ally. Indeed, neither Utah nor Virginia have recognized a common-law duty to protect electronic private information from unauthorized disclosure. *See, e.g.*, *Parker v. Carilion Clinic*, 819 S.E.2d 809, 826 (Va. 2018) (declining to recognize duty); *Deutsche Bank Nat'l Tr. Co. v. Buck*, 2019 WL 1440280, at *5 (E.D. Va. Mar. 29, 2019) (dismissing negligence claim because plaintiff "failed to establish" that Virginia law recognizes a common-law duty to "safeguard private information").[10] Instead, Plaintiff alleges that Ally affirmatively assumed a duty to Plaintiff "[b]y collecting and storing [Plaintiff's] data." Compl. ¶ 62. But neither Utah

[9] In pre-motion letters, Ally and Plaintiff cited Utah and Virginia law for these claims. "[S]uch implied consent is . . . sufficient to establish the applicable choice of law." *Trikona Adv. Ltd. v. Chugh*, 846 F.3d 22, 31 (2d Cir. 2017).

[10] The Utah Supreme Court has not addressed whether Utah recognizes a common-law duty in this context and no federal or other court applying Utah law has found that Utah would recognize such a duty.

nor Virginia state courts have recognized any assumed duty outside the context of negligent actions causing *physical harm*. Indeed, the Supreme Courts of both states have adopted Restatement (Second) of Torts § 323 as the standard for finding an assumed duty, which requires "physical harm resulting from [defendant's] failure to exercise reasonable care to perform his undertaking." *See MacGregor v. Walker*, 322 P.3d 706, 711 (Utah 2014) ("[S]ection 323, by its very terms, requires 'physical harm' from the negligently rendered services."); *Davis v. Walmart Stores E., L.P.*, 687 F. App'x 307, 311 (4th Cir. 2017) (recognizing that "assumption of duty applies only in a narrow subset of Virginia cases: wrongful death, wrongful birth, and one specific type of negligent driving cases").[11] Dispositively, Plaintiff does not allege any physical harm.

Even if Ally assumed a duty under either Utah or Virginia law, Plaintiff does not plausibly allege that Ally failed to use reasonable care. *Harris*, 572 F.3d at 72 ("[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice"). As an initial matter, the mere fact that the Coding Error occurred is insufficient to infer a lack of reasonable care because negligence is not a strict liability standard. *See, e.g.*, *Bylsma v. R.C. Willey*, 416 P.3d 595, 605 (Utah 2017); *Arlington Forest Assoc. v. Exxon Corp.*, 774 F. Supp. 387 (E.D. Va. 1991) (refusing to conflate negligence and strict liability standards). Even the regulatory authorities Plaintiff cites in the Complaint, such as the Federal Trade Commission, acknowledge that data exposures "sometimes can happen when a company has taken every reasonable precaution."[12] Moreover, Plaintiff does not (and cannot) allege that bad actors exploited vulnerabilities in Ally's systems, that the information affected by the Coding Error was disclosed

---

[11] "The Virginia Supreme Court has only relied on the section 323 rationale in wrongful death, wrongful birth, and one specific type of negligent driving cases." *Bosworth v. Vornado Realty L.P.*, 2010 WL 8925838, at *7 (Va. Cir. Ct. Dec. 20, 2010) (collecting cases).

[12] *See* Fed. Trade Comm'n, *FTC Working to Protect Consumers and Businesses from Information Security Breaches* (Apr. 21, 2004), *available at* https://www.ftc.gov/news-events/press-releases/2004/04/ftc-working-protect-consumers-and-businesses-information-security.

to bad actors, that the information was highly sensitive or inherently valuable, or that Ally was aware of but failed to address weaknesses in its systems. *E.g.*, *McCartney v. United States*, 31 F. Supp. 3d 1340, 1346 (D. Utah 2014) (dismissing negligence claim where there was no allegation that defendant "acted unreasonably in its undertaking [of duty]"); *see supra* Section I.B–C.

Instructive of Plaintiff's failure is *In re Capital One Consumer Data Security Breach Litigation*, 488 F. Supp. 3d 374, 400–01 (E.D. Va. 2020), in which the court found—in circumstances wholly unlike those here—that the plaintiff had stated a negligence claim under an assumed duty theory where the defendants (i) solicited potential customers' highly sensitive personal data *and* maintained a "data lake" of that data solely for their own business purposes unconnected with the customer; (ii) were "aware of the vulnerabilities and risks associated with their servers" on which the data was stored; and (iii) "acknowledged and anticipated attempts to gain unauthorized access" to the "data lake" of personal data yet "inadequately" protected against such access. *Id*. at 398–401. *Id*.[13] Plaintiff does not (and cannot plausibly) plead anything analogous here.

2. Plaintiff does not allege legally cognizable damages.

Even if Plaintiff pled either an assumed duty or a lack of reasonable care (he does not), Plaintiff's negligence claim still fails because he does not allege any legally cognizable damages caused by the Coding Error.[14] Plaintiff's only allegations of harm are "lost time, annoyance,

[13] Though recognizing that Virginia has never recognized a assumed duty outside the context of "wrongful death, wrongful birth, or certain driving-related torts," and despite quoting Section 323's "physical harm" requirement, the Eastern District of Virginia found—inconsistent with Virginia law—an assumed duty under the facts of that case, including that defendants had intentionally and knowingly created a vulnerable "data lake" comprised of highly sensitive information. *In re Capital One*, 488 F. Supp. 3d at 400.

[14] "Pleading damages to support a cause of action is distinct from pleading injury-in-fact to support standing" and subject to the higher Rule 12(b)(6) standard. *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *5 (S.D.N.Y. Mar. 23, 2021). Thus, even if "plaintiffs' allegations are sufficient to support standing, plaintiffs must also plead cognizable damages to survive defendant's motion to dismiss under Rule 12(b)(6)." *Id.* at *5 (citing *Doe v. Chao*, 540 U.S. 614, 624–25 (2004)).

interference, and inconvenience," "diminution in value" of his personal information, "three attempts by hacker[s] to reset the password of his email," and alleged risk of *future* injury from fraud or "identity theft crimes." Compl. ¶¶ 31–33, 51, 69. Although Plaintiff's failure to allege physical harm is dispositive (*see supra* Section II.C.1), these alleged harms also fail because they are speculative. Under both Utah and Virginia law, damages must be actual and non-speculative to be cognizable and support a negligence claim. *See, e.g.*, *Seale v. Gowans*, 923 P.2d 1361, 1365 (Utah 1996) (an alleged breach "causing only nominal damages, speculative harm, or the threat of future harm does not suffice to create [a] cause of action for negligence"); *Hunsaker*, 870 P.2d at 897 (Utah negligence law "requires that the plaintiff *in fact* suffered injuries or damages" (emphasis added)); *Giant of Va., Inc. v. Pigg*, 152 S.E.2d 271, 276 (Va. 1967) (damages under Virginia law only "allowed as a recompense for loss or injury actually received"); *Finney v. Clark Realty Capital, LLC*, 2020 WL 6948181, at *6 (E.D. Va. 2020) ("personal injury [or] property damage" required to state negligence claim under Virginia law); *see also, e.g.*, *Shafran v. Harley-Davidson, Inc.*, 2008 WL 763177, at *2 (S.D.N.Y. Mar. 20, 2008) (collecting cases from "courts across the country" recognizing that activities in "the anticipation of future injury that has not materialized" is not a "cognizable injury" for negligence and other claims); *see also generally supra* Section I.B–C. Without actual damages, Plaintiff's negligence claim fails.

D. Plaintiff fails to state a negligence *per se* claim (Count II).

Plaintiff's claim for negligence *per se* is premised on Section 5 of the Federal Trade Commission Act (the "FTCA"), which prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. 45(a)(1); Compl. ¶ 72. Plaintiff alleges that Ally violated the FTCA by "failing to use reasonable measures to protect" Plaintiff's username and password, and that that violation constitutes negligence *per se*. Compl. ¶ 72. Plaintiff's claim fails.

Under Utah law, negligence *per se* applies only in cases involving "dangerous instrumentalities." *See Mitchell v. Wells Fargo Bank*, 355 F. Supp. 3d 1136, 1158 (D. Utah 2018) (dismissing negligence *per se* claim premised on alleged violation of a privacy statute because the claim applies "only in cases involving dangerous instrumentalities" (quoting *Hall v. Warren*, 632 P.2d 848, 851 n.1 (Utah 1981))). "Dangerous instrumentalities" include, for example, "depositing and maintaining dynamite in a city, the operation of a steam railway, and of a street railway"—*i.e.*, instrumentalities "the maintenance or operation of which involved safety of life, limb, and property." *White v. Shipley*, 160 P. 441, 444 (Utah 1916). Indisputably, the FTCA—which was designed to prevent unfair or deceptive acts or trade practices (*see* 15 U.S.C. § 45(a)(1))—does not implicate any analogous "dangerous instrumentality" or involve the "safety of life, limb, and property," and thus cannot form the basis for a negligence *per se* claim under Utah law.

Similarly, under Virginia law, a negligence *per se* claim may only be premised on a statute that is expressly "enacted for public safety." *Collett v. Cordovana*, 772 S.E.2d 584, 589 (Va. 2015). "A statute enacted for public safety generally is designed to afford protection to the public against careless or reckless acts which may result in bodily injury or property damage." *Tidewater Marina Holdings, LC v. Premier Bank, Inc.*, 2015 WL 13801664, at *2 (Va. Cir. Ct. Aug. 7, 2015). The FTCA is not designed to protect against either. Indeed, confronted with the very question of whether a negligence *per se* claim could be premised on Section 5 of the FTCA, a Virginia federal court, applying Virginia law, was unequivocal that the FTCA is not "expressly aimed at protecting public safety." *In re Capital One*, 488 F. Supp. 3d at 408. Dismissing the claim, the court distinguished between public safety statutes (such as firearm regulations) and "statutes aimed at protecting society from fraud and other dishonest conduct," which are "not the type of regulation

that can support a negligence *per se* claim." *Id.* (collecting cases). The FTCA cannot form the basis for a negligence *per se* claim. Plaintiff's claim should be dismissed.

E. Plaintiff fails to state a claim for breach of implied contract (Count III).

Plaintiff claims that because he "paid money for services Ally provided" and "entrusted" his "private information" to Ally, he entered an "implied contract[] with Ally pursuant to which Ally agreed to safeguard and protect" his information." Compl. ¶ 79. The Coding Error, Plaintiff alleges, was a breach of that implied contract. *Id.* ¶ 83.

Under Utah and Virginia law, an implied contract may arise from a course of conduct or "manifestation of mutual assent" between two parties. *See Heideman v. Wash. City*, 155 P.3d 900, 908 (Utah Ct. App. 2007); *Nossen v. Hoy*, 750 F. Supp. 740, 744 (E.D. Va. 1990). To state a claim for breach of an implied contract, Plaintiff must allege all of the elements for an express breach of contract claim: (1) the existence of a legally enforceable contract (based on a course of conduct or "mutual assent"); (2) defendant's breach of that contract; and (3) damages caused by the breach. *See Eleopulos v. McFarland & Hullinger LLC*, 145 P.3d 1157, 1159 (Utah Ct. App. 2006); *Filak v. George*, 594 S.E.2d 610, 619 (Va. 2004). Plaintiff's claim fails.

Plaintiff's attempt to derive an implied contract from the Ally website "policies" (*e.g.*, "keeping accounts and personal information secure is a top priority for us") and "Do It Right" slogan falls far short of establishing an enforceable agreement. *See* Compl. ¶¶ 19–21, 80. These policies and slogan lack specificity in terms and conditions required for an enforceable agreement. Instead, they are general statements about Ally's intentions. *See Heideman*, 155 P.3d at 908 (implied contract requires "an intention to make a bargain with certain terms or terms which reasonably may be made certain"); *Willner v. Dimon*, 2015 WL 12766135, at *4 (E.D. Va. May 11, 2015) (website statements must be "clear, definite, and explicit, and leave[] nothing open for negotiation" to be enforceable). This disposes of Plaintiff's claim.

But even if Ally's website policies and company slogan *could* be enforceable agreements (they are not), and even if Plaintiff *could* adequately allege that the Coding Error was a breach of such agreements (he cannot), Plaintiff's claim still fails because he cannot allege any damages. *See supra* Section I.B–C. Plaintiff alleges no out-of-pocket expenses, nor any other economic damages. *See, e.g.*, *Shively v. Utah Valley Univ.*, 2020 WL 4192290, at *3 (D. Utah July 21, 2020) (dismissing implied contract claim for failure to plead damages because plaintiff was "in the same economic position" absent the alleged breach); *Blick v. Shapiro & Brown, LLP*, 2016 WL 7046842, at *3 (W.D. Va. 2016) (dismissing contract claim where plaintiff "failed to allege facts here indicating that he incurred damages" as a result of the alleged breach).[15] Under either Utah or Virginia law, Plaintiff's failure to plead damages is fatal. *See Shively*, 2020 WL 4192290, at *3 ("damages are an essential element of any Utah contract claim"); *Sunrise Continuing Care, LLC v. Wright*, 671 S.E.2d 132, 136 (Va. 2009) ("Proof of damages is an essential element of a breach of contract claim."). Plaintiff's implied contract claim should be dismissed.

F. Plaintiff fails to allege a violation of the VPIBNA (Count IV).

Plaintiff claims Ally violated the Virginia Personal Information Breach Notification Act ("VPIBNA") because it did not "disclose" the Coding Error in a "timely" manner. Compl. ¶ 90. VPIBNA provides that entities that possess the electronic "personal information" of a Virginia resident must provide notification "without unreasonable delay" of any "breach of the security of its system." Va. Code § 18.2-186.6(B). VPIBNA "authorizes an individual to recover direct economic damages from an entity that has violated this statute." *Id.* § 18.2-186.6(I). Plaintiff's claim fails under the statute's plain language.

[15] Additionally, Plaintiff's allegations of "annoyance," "inconvenience," and "anxiety" (Compl. ¶ 34) do not constitute legally cognizable damages. *See, e.g.*, *Cabaness v. Thomas*, 232 P.3d 486, 508 (Utah 2010); *Jaldin v. ReconTrust Co., N.A.*, 539 F. App'x 97, 102–03 (4th Cir. 2013) (applying Virginia law).

First, the information Plaintiff alleges was disclosed as a result of the Coding Error is not "personal information" under the VPIBNA. The VPIBNA defines "personal information" as "the first name or first initial and last name in combination with and linked to any one or more of the following data elements" when "the data elements are neither encrypted nor redacted":

> 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number.

Va. Code § 18.2-186.6(A). Under the plain terms of the statute, Plaintiff's self-selected username and password do not qualify as "personal information."

Second, Plaintiff's claim also fails because Plaintiff cannot adequately allege the statutory requirement of a "breach." The VPIBNA defines "breach of the security of the system" as:

> [T]he unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud.

Id. An inadvertent exposure, as opposed to a malicious hacking, is not a "breach" under the VPIBNA. Regardless, as discussed *supra* Section I, Plaintiff has not alleged that the Coding Error "has caused" or "reasonably . . . will cause" him to suffer identity theft or fraud.

Third, Plaintiff's claim fails because, even if there had been a "breach of the security of the system" with respect to "personal information" (there was not), Plaintiff cannot plausibly allege that Defendants "unreasonably delay[ed]" in providing notice of the Coding Error. The VPIBNA does not define "unreasonable delay," but courts applying the VPIBNA have found periods of four months between discovery the breach and notice to be unreasonable and one month

to be reasonable. *See In re Capital One*, 2020 WL 5629790, at *25 (four months was unreasonable); *Griffey, et al. v. Magellan Health Inc.*, 2021 WL 4427065, at *14 (D. Ariz. Sept. 27, 2021) (one month was reasonable). The time between Ally's discovery of the Coding Error on April 12, 2021 and Ally's June 11, 2021 notification letter was necessary—and thus reasonable—since Ally had to parse millions of login attempts to identify any affected customers. Decl. ¶¶ 16–17. Plaintiff cannot plausibly allege that it was unreasonable for Ally to identify actually affected accounts before notifying actually affected customers.

Finally, Plaintiff's VPIBNA claim fails because Plaintiff has not alleged "direct economic damages." Indeed, as discussed *supra* Section I, Plaintiff has failed to allege *any* damages (*i.e.*, any injury), let alone *economic* damages, which necessarily requires an expenditure of money. *See Corona v. Sony Pictures Enter., Inc.*, 2015 WL 3916744, at *8 (C.D. Cal. 2015) (dismissing VPIBNA claim because "[w]ithout an allegation of economic damages, the claim fails").

G. Plaintiff fails to state a claim for declaratory or injunctive relief (Count V).

Plaintiff claims he is entitled to injunctive or declaratory relief under the Declaratory Judgment Act (the "DJA"), 28 U.S.C. § 2201, based on speculation that "there is no reason to believe that the Defendants' security practices are any more adequate now" than when the Coding Error occurred. Compl. ¶ 98. Under the DJA, the question is whether "the facts alleged . . . show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment." *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007). Plaintiff's claim falls short of this clear standard.

To obtain declaratory or injunctive relief, Plaintiff must plausibly allege entitlement to relief on an underlying substantive claim. *See, e.g.*, *Chevron Corp. v. Naranjo*, 667 F.3d 232, 244 (2d Cir. 2012) (a request for declaratory relief requires a "valid legal predicate"). Because the Complaint fails to state any claim for relief, *see supra* Section II.A–F, Plaintiff is precluded from

seeking declaratory or injunctive relief. *See Chiste v. Hotels.com L.P.*, 756 F. Supp. 2d 382, 406 (S.D.N.Y. 2010) ("Declaratory judgments and injunctions are remedies, not causes of action.").[16]

Regardless, Plaintiff's claim still fails for lack of standing. "[T]o establish standing to obtain prospective relief, Plaintiff must show a likelihood that he will be injured in the future." *Carver v. City of New York*, 621 F.3d 221, 228 (2d Cir. 2010). Plaintiff cannot do so here for the same reasons described *supra* Section I, including that immediately after discovering the Coding Error, Ally eliminated it and forced a reset of all potentially-affected customers' passwords. *See* Decl. ¶¶ 12–13. Ally also confirmed that all third parties to which the information had potentially been exposed had deleted the data. *Id.* ¶ 14. Moreover, Plaintiff does not allege any injury as to which there is any "likelihood" of being "harmed again in the future in a similar way," nor that Plaintiff faces any likelihood of future injury as a result of the Coding Error. *Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 239 (2d Cir. 2016); *see supra* Section I. Thus, even if he had pled a predicate violation, Plaintiff lacks standing to pursue declaratory or injunctive relief claims.

CONCLUSION

For all these reasons, the Complaint should be dismissed in its entirety with prejudice.[17]

---

[16] Moreover, certain of Plaintiff's claims cannot support injunctive relief as a matter of law. *See Patton v. Experian Data Corp.*, 2018 WL 6190349, at *11 (C.D. Cal. Jan. 23, 2018) ("The injunction remedy does not appear in section 18.2-186.6 [VPIBNA]. Thus, there can be no private right of action for injunctive relief.").

[17] Dismissal with prejudice is appropriate because Plaintiff had an opportunity to amend his Complaint after learning of Defendants' arguments in their pre-motion letter requesting permission to file this motion to dismiss. *See* ECF No. 10; *DigitAlb, Sh.a v. Setplex, LLC*, 284 F. Supp. 3d 547, 556–57 (S.D.N.Y. 2018).

Dated: October 25, 2021
New York, New York

SIMPSON THACHER & BARTLETT LLP

By: /s/ *Brooke E. Cucinella*

Brooke E. Cucinella
Joseph M. McLaughlin
Rachel S. Sparks Bradley
Richard F. Walker
425 Lexington Avenue
New York, New York 10017
Telephone: (212) 455-2000
Facsimile: (212) 455-2502
brooke.cucinella@stblaw.com
jmclaughlin@stblaw.com
rachel.sparksbradley@stblaw.com
richard.walker@stblaw.com

Attorneys for Defendants Ally Bank and Ally Financial Inc.